



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/764,548

01/18/2001

Christopher A. Rygaard

1010722.991103

6480

26379

7590

12/18/2003

GRAY CARY WARE & FREIDENRICH LLP
2000 UNIVERSITY AVENUE
E. PALO ALTO, CA 94303-2248

EXAMINER

D AGOSTA, STEPHEN M

ART UNIT

PAPER NUMBER

2683

DATE MAILED: 12/18/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PATENT DOCKET	
DATE:	<u>December 22, 2003</u>
ACTION:	<u>Resp to OA</u>
DUE:	<u>18 March 2004</u>
DEAD:	<u>18 June 2004</u>

Office Action Summary

Application No.

09/764,548

Applicant(s)

RYGAARD, CHRISTOPHER A.

Examiner

Stephen M. D'Agosta

Art Unit

2683

— The MAILING DATE of this communication appears on the cover sheet with the correspondence address —
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s) ____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 1, 2 6) ☐ Other: --

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: *Reference is made that this application is a CIP of another US patent application, but the application number is missing (see page 1, first sentence under Related Applications heading).*

Appropriate correction is required.

Information Disclosure Statement

1. The information disclosure statement filed 11-21-2001 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because **several of the references shown do not have a publication date listed**. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609 ¶ C(1).

2. The examiner noticed, while reading one of the NIST publications, a reference to a Jumping Beans white paper dated December 1998. Upon visiting the www.jumpingbeans.com website, the examiner determined that this is a website for Aramira corporation which appears to be the assignee of the invention (note signature of Chris Rygaard who is CTO of Aramira Corp. on Small Business Concern Statement). **The examiner would appreciate an explanation as to delay between the white paper publication dated 12/98 and the US filing date of 1/01 with priority requested to 6/00 (which is 2.5 years and 1.5 years respectively after the publication date of the white paper).**

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-20 rejected under 35 U.S.C. 102(a) as being anticipated by Jansen et al. NIST Special Publication 800-19 – Mobile Agent Security (hereafter Jansen).

As per **claims 1, 4, 6, 8, 11**, Jansen teaches a mobile application (MA) security system (title and section 3.2, bottom paragraph on page 9), comprising;

One or more nodes of a peer-to-peer network that are configured to execute a MA (page 2, 2nd paragraph teaches MA hopping from peer to peer, see Figure 1 also).

A central security enforcement node (CSEN) connected to each node for controlling the security of a MA (pages 18-19, Protecting Agents section, 3rd paragraph teaches both central and decentralized server architectures)

The central security enforcement node comprising means for monitoring the security of the MA as it jumps between nodes wherein data about the MA is communicated to the central security enforcement node when the MA is communicated from a first to second node (page 13-14, Protecting the Agent Platform, teaches a "reference monitor" that cannot be bypassed AND pages 18-19, teach central or distributed architecture)

Wherein the security monitoring means further comprises means for detecting unwanted changes in the code associated with the MA when the MA is jumping between hosts (page 5, section 2.2.4, Unauthorized Access teaches "modifying the agent's data or code" AND section 2.3.4, Alteration).

With further regard to claim 4, Jansen teaches security monitoring means comprises preventing a node from transmitting hostile code in a MA to another node (page 3, Denial of Service section 2.1.2, teaches "malicious code" being introduced by

an outside person or by an internal test engineer, etc. AND page 19, top paragraph teaches IBM Aglets prevent receiving platform from accepting agents from an agent platform not defined as a trusted peer).

With further regard to claim 6, Jansen teaches security monitoring means comprises detecting unwanted changes in the state of the MA (page 17, State Appraisal teaches prevention of state corruption/modification).

With further regard to claim 8, Jansen teaches security monitoring means comprises detecting unwanted changes to the itinerary of the MA (page 21, Section 4.2.2, Mutual Itinerary Recording teaches tracking of an agent's itinerary).

With further regard to claim 11, Jansen teaches receiving data about a mobile application via State Appraisal, Path Histories, Proof Carrying Code (pages 16-18) which provides data about the MA (and reads on the claim).

With further regard to claim 13, see claim 1, 4 and 11 rejections above.

With further regard to claim 15, see claim 1, 6 and 11 rejections above.

With further regard to claim 17, see claim 1, 8 and 11 rejections above.

With further regard to claim 20, see claim 1, 4 and 11 rejections above (note that a non-trusted host launching a MA reads on hostile code (and or a Denial of Service Attack), as per claim 4 and is disclosed in Jansen).

As per claims 2 and 12, Jansen teaches claim 1/1 wherein the detecting means further comprises means for storing a copy of each MA when the MA is created by having the creating node send a copy of the MA to the CSEN, means for receiving data about the MA when it is received by another node and means for comparing the code of the MA received by the other node to the stored copy of the MA to determine if changes have been made to the code of the MA (Section 3.2, page 9, 1st paragraph teaches protecting against modification of code, ie. comparing the original to the one received AND section 4.2.2 Mutual Itinerary Recording teaches tracking and comparing the Itinerary list as it traverses the peers – Since Jansen discloses both central and distributed CSEN's (see claim 1 above), this reads on using one stored copy for comparison purposes. Further to this point are the lists/tables, bottom list on page 14

and top list on page 19, which disclose many possible countermeasure means – one skilled in the art would provide for a one-to-one code compare at a minimum).

As per **claim 3**, Jansen teaches claim 1 wherein the detecting means further comprises means for receiving a checksum of the MA when the MA is created, means for receiving the MA after it is sent to another node, means for computing the checksum of the received MA and means for comparing the checksum of the MA after it is received by another node to the stored checksum of the MA to determine if changes have been made to the code of the MA (page 16, Signed Code section teaches digital signature/Authenticode which provides “code signing” to provide means for determining an authentic message or not AND page 17, Path Histories teaches adding a signed entry to the path which is used to verify validity of the MA/message AND page 17-18, Proof Carrying Code section AND pages 19-20, teach Public Key and PRAC which are “cryptographic checksums” and are checked for accuracy. Each reads on “checksum”).

As per **claims 5 and 14**, Jansen teaches claim 4/13 wherein preventing means comprises determining if the node dispatching the mobile application is trusted (pages 18-19, Protecting Agents, teaches trusted peers via IBM Aglets and Claim 3 above teaches Signed Code which infers trust), means for saving the code of the MA and means, when requested by another node, for providing the code for the MA to the requesting node (page 13-14, Protecting Agent Platform section – broadly discloses “trusted communications for MA’s” which inherently includes requesting of MA and transmission of MA) **but is silent on** means for stripping the code from an initially received MA if the host is not trusted.

Jansen teaches identifying a non-trusted machine (see previous claim rejections) and hence many options exist as to how to stay safe from said machine, ie. do not communicate with it, only transmit to it, attempt to re-verify that it is a trusted machine, only communicate with certain machines, strip code. The examiner believes that stripping code is the most harsh of the possibilities since it may be that a network error

occurred or the user entered a bad login/password/certificate/etc. which resulted in the failed trusting operation. The stripping of code should be left to a system administrator.

As per **claims 7 and 16**, Jansen teaches claim 6/15 wherein the detecting means further comprises means for saving a copy of the state of a MA received from a node that received the MA, means for receiving data about the same MA after a jump to another node and means for comparing the state of the MA after the jump to another node with the stored state of the MA to ensure that the state of the MA has not changed (page 17, section 4.1.4, State Appraisal section).

As per **claims 9 and 18**, Jansen teaches claim 8/17 wherein the detecting means further comprises means for saving a copy of the itinerary of a MA received from a node that received the MA, means for receiving the same MA after a jump to another node and means for comparing the itinerary of the MA after the jump to another node with the stored itinerary of the MA to ensure that the itinerary of the MA has not changed (page 21, section 4.2.2, Mutual Itinerary Recording and Itinerary Recording with Replication/Voting sections).

As per **claims 10 and 19**, Jansen teaches claim 8 wherein the itinerary comprises past historical itinerary data (page 17, Path Histories section AND page 21, Mutual Itinerary Recording and Itinerary Recording with Replication/Voting sections).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:


1. T Karygiannis, NIST Pub. Discloses Security testing using mobile agents
2. Takewaki et al. US 6,539,416 discloses managing mobile agents.
3. Walsh US 6,233,601 discloses itinerary-based agent mobility.
4. Suzuki EP0942370 discloses mobile agent operations.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 703-306-5426. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bill Trost can be reached on 703-308-5318. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9314 for regular communications and 703-872-9314 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist on 703-306-0377.

SMD
12-6-03


WILLIAM TROST
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600